機械安全

UL Solutions 在歐洲提供 EC Type和 UKCA 認證服務。我們的全球服務為在地處理商提供歐盟認可的公告機構，目標是遵循機械指令 2006/42/EC 和 ATEX 指令 2014/34/EU。我們提供全面性的服務，內容包括機械、ATEX、電磁相容性以及網路安全。我們的全球市場准入解決方案也讓這些服務更完善，讓客戶可以成功進入全球市場。

ISO 13849：性能識別

ISO 13849 針對評估控制系統 (SRP/CS) 安全相關部分進行類別分類，這些控制系統除了操作功能外，也提供安全功能。ISO 13849 可以協助客戶遵循機械指令 2006/42/EC 附錄 I 的基本健康和安全要求 (EHSR)。SRP/CS 的安全功能可以達到定義為性能等級 (PL) 中的安全完整性。表 3 (ISO 13849) 顯示每小時成正比的危險故障的平均概率和使用 IEC 62061 等效的安全完整性等級 (SIL) 的各種性能等級 (PL)。

ISO 13849 PL	PFH (d) 危險故障/每小時。	IEC 62061 (SIL)
a	≥ 10^{-5} 到 < 10^{-4}	不適用
b	≥ 3×10^{-6} 到 < 10^{-5}	SIL 1
c	≥ 10^{-6} 到 < 3×10^{-6}	SIL 1
d	≥ 10^{-7} 到 < 10^{-7}	SIL 2
e	≥ 10^{-8} 到 < 10^{-7}	SIL 3

表 3：PL 與 IEC 62061 定義的 PFH 和 SIL

五個性能等級 (a、b、c、d 和 e) 與風險程度成正比，其中 (a) 風險最低，(e) 風險最高。如表 4 (ISO 13849) 所示，PL 使用三個主要因子確定：架構類別 (Cat)、診斷覆蓋率 (DCavg) 和 $MTTF_D$ 因子。表 4 提供依據 Cat 2、媒介 DCavg、高 $MTTF_D$ 因子系統的安全性能 (SRP/CS)，然後可以達到 PL (d) 等級。

Cat	B	1	2	2	3	3	4
DCavg	無	無	低	中	低	中	高
$MTTF_D$							
低	a	不適用	a	b	b	c	不適用
中	b	不適用	b	c	c	d	不適用
高	不適用	c	c	d	d	d	e

表 4：確定 PL 的簡化流程

認證功能安全專業人員

我們設計的認證功能安全專業人員計劃 (UL-CFSP)，讓您深入理解工業、汽車和其他產業日常使用的最先進功能安全基本概念。該計劃讓個人可以專注於功能安全的關鍵知識和技能，取得相關的證書，證明自己的能力凌駕於他人之上。UL-CFSP 計劃為初學者和希望深化功能安全方面現有知識和技能的人員有機會展現並獲得該領域的專業證書。

認證功能安全專家

我們的功能安全專家認證 (UL-CFSX) 計劃適用已取得功能安全認證或獲得 CFSP 資格的優質工程師。人員認證授予精通工業功能安全知識和技能的人員。他們必須擁有多年的產業經驗並在相關領域從事功能安全性工作。

功能安全培訓計畫

目前功能安全專案的焦點在於工業流程、汽車、半導體、自動駕駛汽車、機械、工業自動化、網路安全和消費性產品。
其中包括以下標準的適用範圍：ISO 26262、ISO 21448、UL 4600、IEC 61508、IEC 61511、ISO 13849、ISO 10218、IEC 61800-5-2、ISO 25119、ISO 19014、UL/IEC 60730、UL 1998、UL 991、SAE 3061、ISO 21434 和 IEC 62443。

製程產業——IEC 61511

三天的技術培訓 課程中，我們的講師將說明與電子和安全儀表系統相關的製程產業功能安全標準和概念。

功能安全和機械指令

功能安全和機械指令 (MD) 是為期三天的技術培訓課程，內容包括 MD 概念、功能安全標準、風險評估以及與歐盟機械指令相關的安全標準。

汽車產業——ISO 26262

該課程深入探討 ISO 26262:2018 的所有部分，包括第 11 部分。內容包括廣泛的半導體技術和零組件，包括微型控制器、類比和混合訊號設計、可程式編碼邏輯裝置、記憶體和 FMEDA 範例。

TI:EIA22CS290410zhTW

UL Solutions

功能安全要點

在您的產品面對當今工業功能安全方面的挑戰時，UL Solutions 將幫助您披荊斬棘迎向成功。

製程產業

根據 IEC 61508 和 IEC 61511，進行模組和公司功能安全管理的評估和認證，內容包括符合 ATEX 和機械指令的安全相關設備。

根據 IEC 61511，評估 HAZOP、LOPA 並驗證安全儀表系統。

機械安全

根據 IEC 62061 ISO 13849 和 IEC 61800-5-2，評估模組和安全系統，並依據機械指令 2006/42/EC，簽發 EC 和 UKCA 型檢查認證。

功能安全課程訓練

IEC 61508、IEC 61511、IEC 61800-5-2、IEC 62061、ISO 13849、ISO 25119、UL 991/UL 1998、EN 50271 和 UL 60730-1 附錄 H。

提供兩種等級的培訓：

- 認證功能安全專業人員 (CFSP)
- 認證功能安全專家 (CFSX)

聯絡我們，電子郵件： global.functionalsafety@ul.com
UL.com/functionalsafety

Safety. Science. Transformation.™

為什麼選擇 UL Solutions 的工業功能安全解決方案？

UL Solutions 在推動安全和性能以及工業和功能安全進步方面佔有領先的地位。在標準制定方面，UL Solutions 發揮重要的影響力。UL Solutions 是最早進行功能安全的認證機構之一，最早可以追溯到 1994 年，當時的 UL 1998（可程式編程零組件軟體標準）是為配備嵌入式軟體的商業產品而制定。我們持續針對 UL 4600 自主產品評估等最新標準，進行安全性的創新。

UL Solutions 以其在認證和參與標準制定的悠久歷史，成為功能安全合規性方面值得信賴的夥伴。憑藉我們遍佈全球的設施和資源，以及在國際和地區法規方面無與倫比的專業知識，我們有能力在全球範圍內提供安全相關設備的認證和評估，並評估公司在功能安全認證管理方面的能力。

揭開功能安全認證的面紗

各種法規，包括 ATEX 指令，得以提高功能安全合規性。讓所有歐盟成員國的標準趨於一致，如果產品符合要求，則在整個歐盟境內可以被視為具有高安全完整性等級（SIL 等級），進而降低和緩解風險。這些趨於一致的標準直接引用廣為人知的功能安全標準，例如 IEC 61508 等。安全相關標準認證獲得主管機關的認可並被終端用戶接受的事實證明，合規性是成功的不二法門。此外，由公正的第三方專家進行的合規性評估並獲得當地技術主管機關的核准更別具意義。

功能安全的目標

功能安全的重點在於於實作安全儀表系統（SIS），透過分析風險來降低風險。該分析包括 HAZOP 研究，以確定與風險降低因子（RRF）相對程度成反比的安全完整性程度（SIL）。

RRF 可以透過 SIS 達成，如圖 1 所示。SIS 由感應器、邏輯解算器（LS）和最終元件組成，而這些元件可以根據流程產生的需求執行多個 SIF。如果流程達到可以偵測到故障或異常流程的階段，則會啟動需求。

SIL 是由 SIF 執行的風險降低程度的量測值。針對低要求和高要求的安全性功能，可以透過整合形成 SIS 的多個元件或模組執行 SIF，該流程需要符合特定參數，如表 1（IEC 61508）所示的每個實作的 SIF 的定量隨機硬體分析、其回應時間、RRF、可用性和安全等級。

安全儀表系統設計

與任何其他產品一樣，安全相關裝置很容易發現故障。這些可能主要是因為定量分析的隨機硬體和定性測量的系統故障而導致。故障可能是因為安全要求規範未明確定義而造成，至少 45% 的產品故障

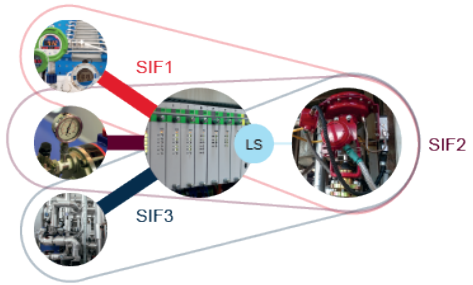

圖 1：多個 SIF 組成 SIS

RRF	PFD_{AVG}（低需求）	PFH (d)，高需求/待續。	目標 SIL
10—100	10^{-2} 到 < 10^{-1}	10^{-6} 到 < 10^{-5}	1
100—1,000	10^{-3} 到 < 10^{-2}	10^{-7} 到 < 10^{-6}	2
1,000—10,000	10^{-4} 到 < 10^{-3}	10^{-8} 到 < 10^{-7}	3
10,000—100,000	10^{-5} 到 < 10^{-4}	10^{-9} 到 < 10^{-8}	4

表 1：SIL 確定與 RRF、PFD 和 PFH

歸因於此；缺乏專案生命週期階段的能力，導致生命週期檔案品質不佳；缺乏可追溯性；或在專案生命週期階段缺少主要安全要求規範的驗證。

兩種評估可以衡量 SIS 的 SIL 能力：每個元素必須進行定量和定性評估。

定量（隨機硬體故障）

在整個設備週期會隨時發生隨機的硬體故障。因為如熱應力、異常應用、感應器疲勞和缺乏驗證測試等因素，會以無法預期的方式隨機發生。

IEC61508:2010 提供兩種達到最高可量化 SIL 的方式：Route 1_H 或 Route 2_H。

Route 1_H 的技術需視 FMEDA 的隨機硬體統計評估而定，該評估會分析每個零組件的功能，以確定故障對安全功能的影響。可以評估該故障屬於安全或危險的安全狀態。Route 2_H 可以用來驗證使用（PIU）評估。

依據現場收集的回應資料，計算安全功能是否屬於危險故障。PIU 適用 A 型（簡單設計）和 B 型（複雜設計）產品。

如圖 2（IEC 61508）所示的隨機硬體故障分佈。

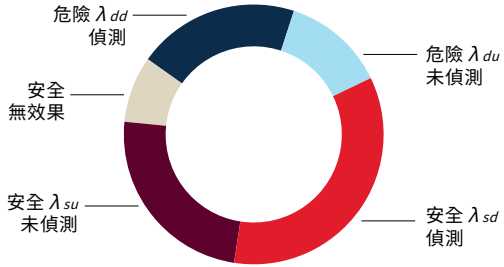

圖 2：隨機硬體故障分佈

安全完整性等級參數

元件安全功能的 SIL 由兩個因子決定：PFD_{AVG}（見表 1）和安全故障失效比率（SFF），如表 2（IEC 61508）所示。

如下計算 SFF 和 PFD：

$$SFF = \frac{\lambda su + \lambda sd + \lambda dd}{\lambda su + \lambda sd + \lambda dd + \lambda du} \qquad PFD = \frac{\lambda du \times Tpti}{2}$$

期中 **Tpti** 是驗證測試間隔

安全故障失效比率 (SFF)	A 類子系統			B 類子系統		
	硬體故障容差值 (HFT)			硬體故障容差值 (HFT)		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	無 SIL	SIL 1	SIL 2
60%—< 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90%—< 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

表 2：A 型或 B 型的架構限制

備註：
更高的安全功能 SIL 須視硬體容差值和產品類型的架構限制而定。